ABSTRACT

A verification technique in which a client verifies a server includes the use of two different digital certificates—one certificate derived from and including the other certificate. One certificate is programmed into the server it is desired to verify. This certificate includes various values that are signed with a secure private key, which may be, for example, the private key of the manufacturer of the server or subsystem within the server. The second certificate is derived from and includes the first certificate. This latter certificate also includes one or more server identity values (*e.g.*, IP address, domain name) and is signed by a second private key that is preferably different than the private key used to sign the first certificate. Both certificates must be verified successfully by a client before a secured communication is permitted to proceed.